

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-353226
(P2000-353226A)

(43) 公開日 平成12年12月19日 (2000. 12. 19)

(51) Int.Cl. ⁷	識別記号	F I	データベース* (参考)
G 0 6 K 19/07		G 0 6 K 19/00	N
17/00		17/00	D
19/00		G 0 9 C 1/00	6 6 0 D
G 0 9 C 1/00	6 6 0	G 0 6 K 19/00	Q
G 1 0 L 19/00		G 1 0 L 9/00	N

審査請求 未請求 請求項の数 7 O L (全 18 頁) 最終頁に続く

(21) 出願番号 特願2000-105007(P2000-105007)

(22) 出願日 平成12年4月6日 (2000. 4. 6)

(31) 優先権主張番号 特願平11-99948

(32) 優先日 平成11年4月7日 (1999. 4. 7)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 岡上 拓己

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 佐々 哲

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082762

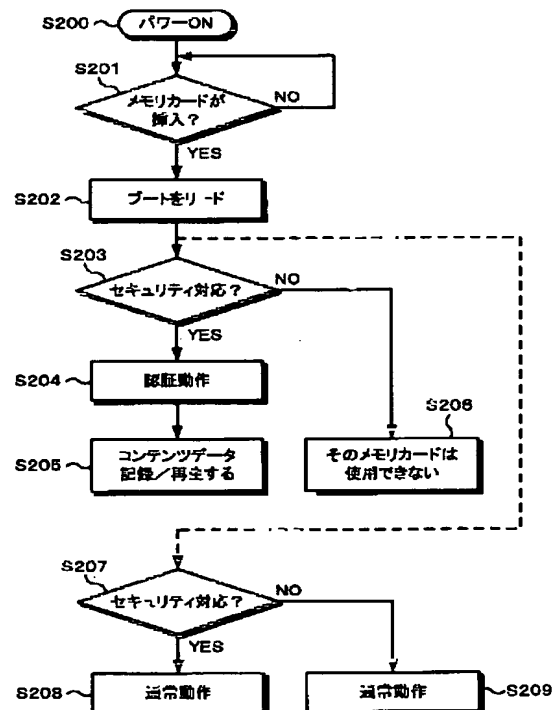
弁理士 杉浦 正知

(54) 【発明の名称】 メモリ装置、データ処理装置および方法

(57) 【要約】

【課題】 セキュリティ機能のような新機能をメモリ装置が持つかどうかを瞬時に決定する。

【解決手段】 機器の電源がオンされると、メモ리카ードが挿入されているかどうか決定され、メモ리카ード中のブートブロックが読み込まれる (ステップ S 2 0 2)。ブートブロック中の識別情報を参照して、挿入されたメモ리카ードがセキュリティ対応か、非対応かが決定される (ステップ S 2 0 3)。セキュリティ対応のメモ리카ードであれば、認証動作がなされ (ステップ S 2 0 4)、認証成立後にコンテンツデータの記録/再生がなされる (ステップ S 2 0 5)。セキュリティ非対応のメモ리카ードの場合には、ステップ S 2 0 6において、そのメモ리카ードが使用できない旨の告知がなされる。若し、機器がセキュリティ非対応の場合には、ステップ S 2 0 7における決定の結果が肯定、否定の何れであっても、ステップ S 2 0 8および S 2 0 9で示すように、メモ리카ードに対して、通常動作を行う。



【特許請求の範囲】

【請求項1】 データ処理装置に対して着脱自在のメモリ装置において、
不揮発性メモリと、

既存のメモリ装置と異なる新機能を実現するための手段と、

データ処理装置と上記不揮発性メモリとの間に配されたインタフェース手段とを備え、

上記不揮発性メモリの記憶領域中で、使用時にデータ処理装置によって最初に読まれる所定の記憶領域に、上記新機能を持つかどうかの識別情報を記録することを特徴とするメモリ装置。

【請求項2】 着脱自在で、不揮発性メモリを含むメモリ装置を記録媒体として使用するデータ処理装置において、

メモリ装置と通信を行うインタフェース手段と、

既存のメモリ装置を使用した場合と異なる新機能を実現するための手段とを備え、

上記メモリ装置を使用する時に、最初に読み込む所定の記憶領域中の識別情報によって、装着されたメモリ装置が上記新機能を有するかどうかを決定するようにしたデータ処理装置。

【請求項3】 請求項1または2において、
上記新機能がセキュリティ機能であることを特徴とするメモリ装置。

【請求項4】 データ処理装置によって、データ処理装置に対して着脱自在のメモリ装置に対して情報の書き込みまたは読み出しを行うデータ処理方法において、
メモリ装置を使用する時に、最初に上記メモリ装置内の不揮発性メモリの所定の記憶領域を読み出すステップと、

上記記憶領域中の識別情報によって、既存のメモリ装置と異なる新機能を上記メモリ装置が有するか否かを決定するステップとからなることを特徴とするデータ処理方法。

【請求項5】 請求項4において、
上記新機能がセキュリティ機能であることを特徴とするデータ処理方法。

【請求項6】 請求項4において、
データ処理装置が上記新機能に対応している時に、
上記メモリ装置が上記新機能を有すると決定される場合に、データの書き込みまたは読み出しを行い、上記メモリ装置が上記新機能を有しないと決定される場合に、データの書き込みまたは読み出しを行わないステップをさらに有することを特徴とするデータ処理方法。

【請求項7】 請求項4において、
データ処理装置が上記新機能に対応していない時に、
上記メモリ装置が上記新機能を有する否かに係わらず、データの書き込みまたは読み出しを行うステップをさらに有することを特徴とするデータ処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、例えばオーディオデータを記録する媒体として、機器に着脱自在のメモリカードを使用するようにしたメモリ装置、データ処理装置および方法に関する。

【0002】

【従来の技術】EEPROM(Electrically Erasable Programmable ROM)と呼ばれる電氣的に書き換え可能な不揮発性メモリは、1ビットを2個のトランジスタで構成するために、1ビット当たりの占有面積が大きく、集積度を高くするのに限界があった。この問題を解決するために、全ビット一括消去方式により1ビットを1トランジスタで実現することが可能なフラッシュメモリが開発された。フラッシュメモリは、磁気ディスク、光ディスク等の記録媒体に代わりうるものとして期待されている。

【0003】フラッシュメモリを機器に対して着脱自在に構成したメモリカードも知られている。このメモリカードを使用すれば、従来のCD(コンパクトディスク)、MD(ミニディスク)等のディスク状媒体に代えてメモリカードを使用するデジタルオーディオ記録/再生装置を実現することができる。

【0004】メモリカードを記録媒体とするオーディオレコーダでは、デジタル記録/再生を行うので、比較的高品質のデータを復元できる圧縮方式を使用している場合には、記録/再生される曲等の著作権を保護する必要がある。その方法の一つとして、暗号化技術によって、真正なメモリカード以外のメモリカードを使用不可能とする方法がある。すなわち、真正なレコーダと真正なメモリカードの組み合わせによって、暗号化を復号化することを可能とするものである。また、著作権保護に限らず、メモリカードに格納された情報の機密性が必要のために暗号化技術を採用する場合もある。

【0005】従来のメモリカードは、それ自体に暗号化の機能を持っていなかった。従って、機密性の必要なデータをメモリカードに記録しようとする場合、セット側においてデータを暗号化し、暗号化されたデータをメモリカードに記録することが必要とされる。しかしながら、復号化のキーをメモリカード上に格納する場合には、機密性が保たれない。一方、復号化のキーをセット内にとどめた場合には、暗号化されたデータをそのセット以外に復号化することができず、メモリカードの互換性を保てない問題がある。例えば自分のセットで記録したメモリカードを他人のセットでは、復号できない。この問題を解決するために、セットおよびメモリカードの両者が暗号化の機能を持ち、相互認証を行うことによって、機密性とカードの互換性を確保することが提案されている。

【0006】実際には、著作権保護が不要なデータをメ

メモリカードに記録／再生することがある。例えば会話を記録するような場合には、オーディオ圧縮方式としては、復元される音声の品質が比較的悪くても、圧縮率が高いものが使用される。この場合には、著作権保護は、不要である。また、電子スチルカメラ、ビデオカメラ等で撮影した画像を記録する媒体としてメモリカードを使用する場合も、著作権保護が不要である。一般的に暗号化の機能を持つ、セキュリティ対応のメモリカードは、それを持たないメモリカード、すなわち、従来型のメモリカードに比してコストが高く、高価なものとなる。従って、著作権保護、機密性の保持の必要性に応じて、セキュリティ対応のメモリカードと、非対応のメモリカードを利用することが予想される。

【0007】セットおよびメモリカードがそれぞれセキュリティ対応と、非対応の2種類存在する場合、まず、セキュリティ機能を動作させ、正常な動作がなされるか、エラーになるのかによって、セキュリティ対応、セキュリティ非対応を決定する必要がある。他の方法では、メモリカードの形状を機能の相違に応じて異ならせるようになされる。例えば切欠の有無で区別し、セキュリティ機能を有するメモリカードは、セキュリティ非対応のメモリカードを使用する下位の機器に装着不可能とするようになされる。

【0008】

【発明が解決しようとする課題】セキュリティ機能を持つかどうかを決定する時に、セキュリティ機能を実際に動作させる方法は、エラーとなる場合には、その動作が無駄となり、また、無駄な動作により遅延が生じ、利用者にとって快適な操作環境とはいえない問題がある。また、形状で区別する方法は、機器とメモリカードの対応関係が一義的に決まってしまう、例えばセキュリティ機能を有するメモリカードを、セキュリティ機能が発揮されないけれども、下位の機器で使用する可能性をなくしてしまう問題がある。すなわち、セキュリティ非対応のセットが既に存在している場合には、既存のセットによってセキュリティ対応のメモリカードを使用できることが望まれる。例えば、セキュリティ非対応のハンディムービー（カメラ一体型の記録再生機）が撮影した画像をセキュリティ対応のメモリカードに記録し、メモリカードから再生できることが望まれる。この場合には、暗号化の機能が使用されない。

【0009】従って、この発明の目的は、上述した問題を生じることなく、メモリ装置が既存のものとは異なる新機能を持つかどうかを決定することができるメモリ装置、データ処理装置および方法を提供することにある。

【0010】

【課題を解決するための手段】上述した課題を解決するために、請求項1の発明は、データ処理装置に対して着脱自在のメモリ装置において、不揮発性メモリと、既存のメモリ装置と異なる新機能を実現するための手段と、

データ処理装置と不揮発性メモリとの間に配されたインタフェース手段とを備え、不揮発性メモリの記憶領域中で、使用時にデータ処理装置によって最初に読まれる所定の記憶領域に、新機能を持つかどうかの識別情報を記録することを特徴とするメモリ装置である。

【0011】請求項2の発明は、着脱自在で、不揮発性メモリを含むメモリ装置を記録媒体として使用するデータ処理装置において、メモリ装置と通信を行うインタフェース手段と、既存のメモリ装置を使用した場合と異なる新機能を実現するための手段とを備え、メモリ装置を使用する時に、最初に読み込む所定の記憶領域中の識別情報によって、装着されたメモリ装置が新機能を有するかどうかを決定するようにしたデータ処理装置である。

【0012】請求項4の発明は、データ処理装置によって、データ処理装置に対して着脱自在のメモリ装置に対して情報の書き込みまたは読み出しを行うデータ処理方法において、メモリ装置を使用する時に、最初にメモリ装置内の不揮発性メモリの所定の記憶領域を読み出すステップと、記憶領域中の識別情報によって、既存のメモリ装置と異なる新機能をメモリ装置が有するか否かを決定するステップとからなることを特徴とするデータ処理方法である。

【0013】この発明では、メモリ装置を使用する時に、最初に読み出される不揮発性メモリの領域に、新機能を持つかどうかの識別情報を記録する。データ処理装置は、この識別情報から直ちにメモリ装置が新機能を持つかどうかを設定することができる。

【0014】

【発明の実施の形態】以下、この発明の一実施形態について説明する。図1は、この発明の一実施形態の全体の構成を示す。この一実施形態は、記録媒体として、着脱自在のメモリカードを使用するデジタルオーディオ信号のレコーダ（記録および再生機）である。図1において、破線が囲んで示す1がセットとしてのレコーダを示し、40がレコーダに着脱自在のメモリカードを示す。なお、この発明は、デジタルオーディオ信号以外に動画データ、静止画データ等の記録／再生に対しても適用できる。

【0015】レコーダ1は、CPU2と、CPU2とバスで接続されたセキュリティブロックと、操作ボタン4と、表示デバイス5とを有している。セキュリティブロック3は、DES(Data Encryption Standard)の暗号化回路を含む。操作ボタン4からのユーザの操作に応じて発生した録音指令、再生指令等のデータがバスを介してCPU2に与えられる。種々の情報、レコーダ1の動作状態等が表示デバイス5によって表示される。さらに、6は、外部入出力と内部のオーディオエンコーダ／デコーダ7との間に設けられたオーディオインターフェースである。

【0016】後述するように、メモリカード40は、フ

ラッシュメモリ（不揮発性メモリ）42、DESの暗号化回路を含むセキュリティブロック52、通信用インターフェース、レジスタ等が1チップ上にIC化されたものである。メモリカード40は、レコーダ1に対して着脱自在とされている。なお、この一実施形態では、暗号化機能を有しないメモリカード、すなわち、セキュリティブロックを有しないメモリカードをレコーダ1が使用することが可能とされている。

【0017】オーディオエンコーダ／デコーダ7は、デジタルオーディオ信号を高効率符号化し、また、高効率符号化データを復号する。高効率符号化方法としては、ミニディスクで採用されているATRAC (Adaptive Transform Acoustic Coding)を改良したもの（ATRAC3と表記する）が使用できる。ATRAC3では、44.1kHzでサンプリングした1サンプル16ビットのオーディオデータを処理する。ATRAC3でオーディオデータを処理する時の最小のデータ単位がサウンドユニットSUである。1SUは、1024サンプル分（1024×16ビット×2チャンネル）を数百バイトに圧縮したものであり、時間にして約2.3m秒である。ATRAC3により約1/10にオーディオデータが圧縮される。ミニディスクにおいてそうであるように、ATRAC3の工夫された信号処理によって、圧縮／伸長処理による音質の劣化は少ない。

【0018】MD（ミニディスク）の再生出力、チューナの出力、テープ再生出力等のアナログオーディオ信号8がA/D変換器9によりデジタルオーディオ信号へ変換され、デジタルオーディオ信号がオーディオインターフェース6に供給される。デジタル入力10は、MDまたはCD（コンパクトディスク）の再生出力、デジタル放送、ネットワークで配信されたオーディオデータ等である。デジタル入力10がオーディオインターフェース6に供給される。デジタル入力10は、例えば光ケーブルを介して伝送される。オーディオインターフェース6では、入力選択の処理がされ、選択された入力デジタルオーディオ信号がオーディオエンコーダ／デコーダ7に供給される。

【0019】オーディオエンコーダ／デコーダ7からの符号化データがセキュリティブロック3において暗号化される。セキュリティブロック3は、コンテンツ（ここでは、デジタルオーディオ信号）の著作権を保護するための備えられている。レコーダ1のセキュリティブロック3は、複数のマスターキーと機器毎にユニークなストレージキーを持つ。さらに、乱数発生回路を持ち、セキュリティブロック52を内蔵するメモリカード40が装着された時に、装着されたものが真正なものであるかを確認する認証を行い、正しく認証できれば、セッションキーを共有することができる。

【0020】セキュリティブロック3からの暗号化されたオーディオデータがCPU2に供給される。CPU2

は、着脱機構（図示しない）に装着されたメモリカード40とメモリインタフェース11を介しての通信を行い、暗号化されたデータをメモリカード40のフラッシュメモリ42に書き込む。メモリインタフェース11によって、CPU2とメモリカード40の間では、シリアル通信がなされる。

【0021】CPU2およびメモリインタフェース11によってメモリカード40から読み出した暗号化されたオーディオデータは、セキュリティブロック3によって復号化され、オーディオエンコーダ／デコーダ7によって復号化処理を受ける。オーディオエンコーダ／デコーダ7の出力がオーディオインターフェース6を介してD/A変換器12に供給され、アナログオーディオ出力13へ変換される。また、オーディオエンコーダ／デコーダ7からのオーディオデータ、並びにセキュリティブロック3からの復号化データがインターフェース6を介してデジタル出力14および15として出力される。

【0022】図2は、メモリカード40の構成を示す。メモリカード40は、コントロールブロック41とフラッシュメモリ42が1チップICとして構成されたものである。レコーダ1のCPU2とメモリカード40との間の双方向シリアルインタフェース（メモリインタフェース11）は、10本の線からなる。主要な4本の線は、データ伝送時にクロックを伝送するためのクロック線SCKと、ステータスを伝送するためのステータス線SBSと、データを伝送するデータ線DIO、インタラプト線INTとである。その他に電源供給用線として、2本のGND線および2本のVCC線が設けられる。2本の線Reservは、未定義の線である。

【0023】クロック線SCKは、データに同期したクロックを伝送するための線である。ステータス線SBSは、メモリカード40のステータスを表す信号を伝送するための線である。データ線DIOは、コマンドおよび暗号化されたオーディオデータを入出力するための線である。インタラプト線INTは、メモリカード40からレコーダ1のCPU2に対しての割り込みを要求するインタラプト信号を伝送する線である。メモリカード40を装着した時にインタラプト信号が発生する。但し、この一実施形態では、かかるインタラプト信号をデータ線DIOを介して伝送するようにしているので、インタラプト線INTを接地し、使用していない。

【0024】コントロールブロック41のシリアル／パラレル変換・パラレル／シリアル変換・インタフェースブロック（S/P、P/S、IFブロックと略す）43は、上述した複数の線を介して接続されたレコーダ1のメモリインタフェース11とコントロールブロック41とのインタフェースである。S/P、P/S、IFブロック43は、レコーダ1から受け取ったシリアルデータをパラレルデータに変換し、コントロールブロック41に取り込み、コントロールブロック41からのパラレル

データをシリアルデータに変換してレコーダ1に送る。また、S/P、P/S、IFブロック43は、データ線DIOを介して伝送されるコマンドおよびデータを受け取った時に、フラッシュメモリ42に対する通常のアクセスのためのコマンドおよびデータと、暗号化に必要なコマンドおよびデータとを分離する。

【0025】つまり、データ線DIOを介して伝送されるフォーマットでは、最初にコマンドが伝送され、その後データが伝送される。S/P、P/S、IFブロック43は、コマンドのコードを見て、通常のアクセスに必要なコマンドおよびデータか、暗号化に必要なコマンドおよびデータかを判別する。この判別結果に従って、通常のアクセスに必要なコマンドをコマンドレジスタ44に格納し、データをページバッファ45およびライトレジスタ46に格納する。ライトレジスタ46と関連してエラー訂正符号化回路47が設けられている。ページバッファ45に一時的に蓄えられたデータに対して、エラー訂正符号化回路47がエラー訂正符号の冗長コードを生成する。

【0026】コマンドレジスタ44、ページバッファ45、ライトレジスタ46およびエラー訂正符号化回路47の出力データがフラッシュメモリインタフェースおよびシーケンサ（メモリI/F、シーケンサと略す）51に供給される。メモリI/F、シーケンサ51は、コントロールブロック41とフラッシュメモリ42とのインタフェースであり、両者の間のデータのやり取りを制御する。メモリI/F、シーケンサ51を介してデータがフラッシュメモリ42に書き込まれる。

【0027】フラッシュメモリ42から読み出されたデータがメモリI/F、シーケンサ51を介してページバッファ45、リードレジスタ48、エラー訂正回路49に供給される。ページバッファ45に記憶されたデータがエラー訂正回路49によってエラー訂正がなされる。エラー訂正がされたページバッファ45の出力およびリードレジスタ48の出力がS/P、P/S、IFブロック43に供給され、上述したシリアルインタフェースを介してレコーダ1のCPU2に供給される。

【0028】著作権保護のために、レコーダ1のセキュリティIC40とメモリカード40のセキュリティブロック52とによって、フラッシュメモリ42に書き込まれるコンテンツ（ATRA C3により圧縮されたオーディオデータ、以下ATRA C3データと表記する）は、暗号化される。セキュリティブロック52は、バッファメモリ53、DESの暗号化回路54、不揮発性メモリ55等を有する。

【0029】なお、50は、メモリカード40のバージョン情報、各種の属性情報等が格納されているコンフィグレーションROMである。また、メモリカード40には、ユーザが必要に応じて操作可能な誤消去防止用のスイッチ60が備えられている。このスイッチ60が消去

禁止の接続状態にある場合には、フラッシュメモリ42を消去することを指示するコマンドがレコーダ1側から送られてきても、フラッシュメモリ42の消去が禁止される。さらに、61は、メモリカード40の処理のタイミング基準となるクロックを発生する発振器である。

【0030】メモリカード40のセキュリティブロック52は、複数の認証キーとメモリカード毎にユニークなストレージキーを持つ。不揮発性メモリ55は、暗号化に必要なキーを格納するもので、外部からは見えない。例えばストレージキーが不揮発性メモリ55に格納される。さらに、乱数発生回路を持ち、専用（ある決められたデータフォーマット等の使用が同じシステム内の意味）レコーダ1と正しく認証ができ、セッションキーを共有できる。ATRA C3データを暗号化するためのコンテンツキーは、セッションキーで暗号化されてレコーダ1とメモリカード40との間で伝送される。メモリカード40のセキュリティブロック52と同様に、レコーダ1のセキュリティブロック3もセット固有のストレージキーを有する。暗号化されたコンテンツを移動する時に、ストレージキーを使用してコンテンツキーが掛け直される。

【0031】図3は、暗号化機能を有しない（すなわち、セキュリティ非対応）メモリカード40'を示す。図2に示し、上述したメモリカード40と比較すると、S/P、P/S、IFブロック43に対して、セキュリティブロック52が接続されていない。その他の構成に関して、メモリカード40と40'とは同一である。また、形状、サイズもメモリカード40と40'とが同一とされている。図1に示すレコーダ1は、セキュリティ対応のものであるので、メモリカードとの相互認証、キーの通信等を行う。若し、セキュリティに対応していない図3に示すメモリカード40'を装着すると、レコーダ1は、メモリカード40'がセキュリティ非対応のもので、メモリカード40'を使用できないものと決定する。

【0032】レコーダ1がメモリカードの種類を決定する方法としては、幾つかのものを利用できる。一つの方法では、メモリカードを装着した時に、認証を行うために、キーを伝送する時に、メモリカード40'からは、正規の応答を受信できず、レコーダ1においてタイムアウトの決定がされ、その結果、メモリカードがセキュリティ非対応のもので決定できる。他の方法では、メモリカードを装着した時に、最初にレコーダ1に読み込まれるメモリカードの領域（ブート領域）中に、セキュリティ対応/非対応の識別情報を記録しておき、この識別情報に基づいてレコーダ1がメモリカードの種類を決定することができる。

【0033】また、図1に示すレコーダ1に限らず、セキュリティ非対応のメモリカード40'を使用するようにした機器も存在する。例えばCCDカメラで撮影した

画像をメモリカードに記録し、メモリカードから撮影画像を再生する機能を有する、デジタルハンディムービーは、メモリカード40'を使用できる。かかるデジタルハンディムービーは、セキュリティ対応のメモリカード40を使用できないのが普通である。後述するように、この発明の一実施形態では、メモリカード40の互換性を高めるために、セキュリティ非対応のデジタルハンディムービーのようなセットがメモリカード40を使用した記録および再生ができるように、メモリカード40が構成されている。すなわち、上述したように、S/P、P/S、IFブロック43は、フラッシュメモリ42に対して書き込み/読み出し用のコマンドおよびデータと、セキュリティブロックに必要なコマンドおよびデータとを分離する機能を有している。

【0034】上述したこの発明の一実施形態についてさらに詳細に説明する。図4は、メモリカードを記憶媒体とするコンピュータシステムのファイルシステム処理階層を示す。ファイルシステム処理階層としては、アプリケーション処理層が最上位であり、その下に、ファイル管理処理層、論理アドレス管理層、物理アドレス管理層、フラッシュメモリアクセスが順次おかれる。この階層構造において、ファイル管理処理層がFATファイルシステムである。物理アドレスは、フラッシュメモリの各ブロックに対して付されたもので、ブロックと物理アドレスの対応関係は、不変である。論理アドレスは、ファイル管理処理層が論理的に扱うアドレスである。

【0035】図5は、メモリカード40におけるフラッシュメモリ42のデータの物理的構成の一例を示す。フラッシュメモリ42は、セグメントと称されるデータ単位が所定数のブロック（固定長）へ分割され、1ブロックが所定数のページ（固定長）へ分割される。フラッシュメモリ42では、ブロック単位で消去が一括して行われ、書き込みと読み出しは、ページ単位で一括して行われる。各ブロックおよび各ページは、それぞれ同一のサイズとされ、1ブロックがページ0からページmで構成される。1ブロックは、例えば8KB（Kバイト）バイトまたは16KBの容量とされ、1ページが512Bの容量とされる。フラッシュメモリ42全体では、1ブロック=8KBの場合で、4MB（512ブロック）、8MB（1024ブロック）とされ、1ブロック=16KBの場合で、16MB（1024ブロック）、32MB（2048ブロック）、64MB（4096ブロック）の容量とされる。

【0036】1ページは、512バイトのデータ部と16バイトの冗長部とからなる。冗長部の先頭の3バイトは、データの更新に応じて書き換えられるオーバーライト部分とされる。3バイトの各バイトに、先頭から順にブロックステータス、ページステータス、更新ステータスが記録される。冗長部の残りの13バイトの内容は、原則的にデータ部の内容に応じて固定とされる。13バ

イトは、管理フラグ（1バイト）、論理アドレス（2バイト）、フォーマットリザーブの領域（5バイト）、分散情報ECC（2バイト）およびデータECC（3バイト）からなる。分散情報ECCは、管理フラグ、論理アドレス、フォーマットリザーブに対する誤り訂正用の冗長データであり、データECCは、512バイトのデータに対する誤り訂正用の冗長データである。

【0037】管理フラグとして、システムフラグ（その値が1：ユーザブロック、0：ブートブロック）、変換テーブルフラグ（1：無効、0：テーブルブロック）、コピー禁止指定（1：OK、0：NG）、アクセス許可（1：free、0：リードプロテクト）の各フラグが記録される。

【0038】先頭の二つのブロック0およびブロック1がブートブロックである。ブロック1は、ブロック0と同一のデータが書かれるバックアップ用である。ブートブロックは、カード内の有効なブロックの先頭ブロックであり、メモリカードを機器に装填した時に最初にアクセスされるブロックである。残りのブロックがユーザブロックである。ブートブロックの先頭のページ0にヘッダ、システムエントリ、ブート&アトリビュート情報が格納される。ページ1に使用禁止ブロックデータが格納される。ページ2にCIS(Card Information Structure)/IDI(Identify Drive Information)が格納される。

【0039】図6は、ブートブロックのフォーマットを示す。ブートブロックのヘッダ（368バイト）には、ブートブロックID、フォーマットバージョン、ブートブロック内の有効なエントリ数が記録される。システムエントリ（48バイト）には、使用禁止ブロックデータの開始位置、そのデータサイズ、データ種別、CIS/IDIのデータ開始位置、そのデータサイズ、データ種別が記録される。

【0040】図7は、ブート&アトリビュート情報（968バイト）を詳細に示す。ブート&アトリビュート情報には、メモリカードのクラス、タイプ（読み出し専用、リードおよびライト可能、両タイプのハイブリッド等）、ブロックサイズ、ブロック数、総ブロック数、セキュリティ対応か否か、カードの製造に関連したデータ（製造年月日等）等が記録される。セットは、このセキュリティ対応か否かの識別情報（1バイト）によって、装着されたメモリカードがセキュリティ対応か否かを決定できる。図7において、（*1）が付された情報は、セット側が読み出して装着時に確認する項目であり、（*2）が付された情報は、製造および品質管理上の情報を設定する項目である。

【0041】フラッシュメモリは、データの書き換えを行うことにより絶縁膜の劣化を生じ、書き換え回数が制限される。従って、ある同一の記憶領域（ブロック）に対して繰り返し集中的にアクセスがなされることを防止

する必要がある。従って、ある物理アドレスに格納されているある論理アドレスのデータを書き換える場合、フラッシュメモリのファイルシステムでは、同一のブロックに対して更新したデータを再度書き込むことはせずに、未使用のブロックに対して更新したデータを書き込むようになされる。その結果、データ更新前における論理アドレスと物理アドレスの対応関係が更新後では、変化する。このような処理（スワップ処理と称する）を行うことで、同一のブロックに対して繰り返して集中的にアクセスがされることが防止され、フラッシュメモリの寿命を延ばすことが可能となる。

【0042】論理アドレスは、一旦ブロックに対して書き込まれたデータに付随するので、更新前のデータと更新後のデータの書き込まれるブロックが移動しても、FATからは、同一のアドレスが見えることになり、以降のアクセスを適正に行うことができる。スワップ処理により論理アドレスと物理アドレスとの対応関係が変化するので、両者の対応を示す論理-物理アドレス変換テーブルが必要となる。このテーブルを参照することによって、FATが指定した論理アドレスに対応する物理アドレスが特定され、特定された物理アドレスが示すブロックに対するアクセスが可能となる。

【0043】論理-物理アドレス変換テーブルは、CPU2によってメモリ上に格納される。若し、RAM容量が少ない時は、フラッシュメモリ中に格納することができる。このテーブルは、概略的には、昇順に並べた論理アドレス（2バイト）に物理アドレス（2バイト）をそれぞれ対応させたテーブルである。フラッシュメモリの最大容量を128MB（8192ブロック）としているので、2バイトによって8192のアドレスを表すことができる。また、論理-物理アドレス変換テーブルは、セグメント毎に管理され、そのサイズは、フラッシュメモリの容量に応じて大きくなる。例えばフラッシュメモリの容量が8MB（2セグメント）の場合では、2個のセグメントのそれぞれに対して2ページが論理-物理アドレス変換テーブル用に使用される。論理-物理アドレス変換テーブルを、フラッシュメモリ中に格納する時には、上述した各ページの冗長部における管理フラグの所定の1ビットによって、当該ブロックが論理-物理アドレス変換テーブルが格納されているブロックか否かが指示される。

【0044】上述したメモリカードは、ディスク状記録媒体と同様にパーソナルコンピュータのFATファイルシステムによって使用可能なものである。図5には示されていないが、フラッシュメモリ上にIPL領域、FAT領域およびルート・ディレクトリ領域が設けられる。IPL領域には、最初にレコーダのメモリにロードすべきプログラムが書かれているアドレス、並びにメモリの各種情報が書かれている。FAT領域には、ブロック（クラスタ）の関連事項が書かれている。FATには、未使

用のブロック、次のブロック番号、不良ブロック、最後のブロックをそれぞれ示す値が規定される。さらに、ルートディレクトリ領域には、ディレクトリエントリ（ファイル属性、更新年月日、開始クラスタ、ファイルサイズ等）が書かれている。

【0045】さらに、この一実施形態では、上述したメモリカード40のフォーマットで規定されるファイル管理システムとは別個に、音楽用ファイルに対して、ファイル管理情報（トラック情報管理ファイル）を規定している。トラック情報管理ファイルは、メモリカード40のユーザブロックを利用してフラッシュメモリ42上に記録される。それによって、メモリカード40上のFATが壊れても、ファイルの修復を可能とできる。

【0046】トラック情報管理ファイルは、CPU2により作成される。例えば最初に電源をオンした時に、メモリカード40が装着されているか否かが判定され、メモリカードが装着されている時には、フラッシュメモリ42のブートブロックがCPU2に読み込まれる。ブートブロック中の識別情報によって、装着したメモリカードがセキュリティ対応か、非対応かが決定される。セキュリティ対応であると決定されると、認証動作がなされる。その他のメモリカード40から読み込まれたデータは、CPU2が管理するメモリ（図示せず）に格納される。ユーザが購入して初めて使用するメモリカードでも、出荷時にフラッシュメモリ42には、FATや、ルートディレクトリの書き込みがなされている。トラック情報管理ファイルは、録音がなされると、作成される。認証が成立すると、レコーダ1によって、暗号化されたATRAC3データファイルが記録／再生される。

【0047】記録時には、操作ボタン4で録音ボタンを押すことによって発生した録音指令がCPU2に与えられる。そして、入力したオーディオデータがエンコーダ／デコーダ7によって圧縮され、エンコーダ／デコーダ7からのATRAC3データがセキュリティブロック3により暗号化される。CPU2が暗号化されたATRAC3データをメモリカード40のフラッシュメモリ42に記録する。この記録後にFATおよびトラック情報管理ファイルが更新される。ファイルの更新の度、具体的には、オーディオデータの記録を開始し、記録を終了する度に、CPU2が制御するメモリ（図示せず）上でFATおよびトラック情報管理ファイルが書き換えられる。そして、メモリカード40を外す時に、またはパワーをオフする時に、メモリからメモリカード40のフラッシュメモリ42上に最終的なFATおよびトラック情報管理ファイルが格納される。この場合、オーディオデータの記録を開始し、記録を終了する度に、フラッシュメモリ42上のFATおよびトラック情報管理ファイルを書き換えても良い。編集を行った場合も、トラック情報管理ファイルの内容が更新される。

【0048】上述したこの発明の一実施形態におけるセ

セキュリティ保護機能についてさらに説明する。最初に図8を参照してコンテンツにおけるキーの関係について説明する。メモリカード40のフラッシュメモリ42上では、図8Aに示すように、キーエリア101が設けられ、キーエリア101にコンテンツ（暗号化されたオーディオデータのトラック（曲））毎に作成されるコンテンツキーCKがメモリカードに固有のストレージキーKstmで暗号化されて格納されている。暗号化は、DESと表記され、コンテンツキーCKをストレージキーKstmで暗号化した場合には、DES(Kstm, CK)と表記される。この一実施形態では、暗号化した値は、56ビットにエラー検出用のCRC（8ビット）を加えた64ビット長で扱われる。

【0049】コンテンツのトラック内にパーツデータエリア102が規定され、パーツキーPKがパーツ毎に記録される。パーツは、16Kバイトのブロック103の集合であり、各ブロックには、ブロックシードBK、SEED、イニシャルベクターINVが記録されている。パーツキーPKは、コンテンツを暗号化するブロックキーBKを作成するために、コンテンツキーCKとペアで使用されるものである。すなわち、 $BK = DES(CK(+)PK, BK, SEED)$ （56ビット+8ビット）である。（+）は、排他的論理和を表す。イニシャルベクターINVは、ブロックの暗号化、復号化の初期値である。

【0050】図8Bは、レコーダ1内におけるコンテンツを示す。キーエリア111にコンテンツ毎のコンテンツキーCKが復号化され、レコーダ1に固有のストレージキーKstdで再暗号化されて保持される。すなわち、復号化は、 $IDES(Kstm, CK)$ （56ビット+8ビット）と表記され、再暗号化は、 $DES(Kstd, CK)$ （56ビット+8ビット）表記される。コンテンツを構成するパーツデータエリア112毎にブロックキーBKを作成するためのパーツキーPKが記録される。パーツを構成するブロック113のそれぞれには、ブロックシードBK、SEED、イニシャルベクターINVが記録されている。メモリカード上と同様に、ブロックキーBKは、 $BK = DES(CK(+)PK, BK, SEED)$ （56ビット+8ビット）である。

【0051】図9は、録音時の暗号化の処理の流れを説明するために、簡略化したブロック図であり、図1と対応する部分には、同一符号を付して示し、暗号化の説明に特に不要な構成は、省略されている。Sekは、認証成立時にレコーダ1とメモリカード40との間で共有されるセッションキーである。また、デジタルオーディオ入力10のソースとしてCD10'が示されている。

【0052】メモリカード40がレコーダ1に装着されると、装着したメモリカードがセキュリティ対応のものがどうかブート領域中の識別情報によって決定される。セキュリティ対応のものと決定されると、レコーダ

1とメモリカード40との間で、相互に正規のものであるかを認証する。

【0053】図10は、認証時のセット（レコーダ1）およびメモリカード40間の暗号化の処理を示すものである。最初のステップS1において、メモリカード40のセキュリティブロック52内の乱数発生器によって乱数Rmを発生し、メモリカード40のシリアル番号IDと共に送信する。

【0054】レコーダ1では、ステップS2の処理を行う。すなわち、RmとIDとを受け取り、 $IKj = MAC(MKj, ID)$ の関係にしたがって、認証キーIKjを生成する。MKjは、レコーダ1のセキュリティブロック3に記憶されている複数のマスターキーMK₀ ~ MK₃₁の内では選択された一つのマスターキーである。レコーダ1は、乱数Rdを発生し、認証キーでメッセージ認証子MAC_A（Message Authentication Code）、すなわち、 $MAC(IKj, ID//Rm//Rd)$ を作成する。ここで、A//Bは、AとBの連結（nビットのAの後ろにmビットのBを結合して（n+m）ビットとしたもの）を示す。そして、レコーダ1が乱数Sdを発生し、 $Rd//Sd//MAC_A//j$ をメモリカード40へ送信する。

【0055】メモリカード40は、ステップS3において、このデータRd//Sd//MAC_A//jを受け取り、jからセキュリティブロック52内の認証キーIKjを見つけ、認証キーIKjおよびRd、Rm、IDを用いてMAC_Bを計算する。計算したMAC_Bが受け取ったMAC_Aと同一であれば、メモリカード40は、正しいとしてセット（レコーダ）を認める。そして、ステップS4において、メモリカード40は、 $MAC_C = MAC(IKj, Rm//Rd)$ を作成し、乱数Smを発生する。その後、メモリカード40は、 $Sm//MAC_C$ をレコーダ1に送信する。

【0056】ステップS5において、レコーダ1は、 $Sm//MAC_C$ を受け取る。レコーダ1は、IKj、Rm、Rdを用いてMAC_Dを計算する。計算したMAC_Dが受け取ったMAC_Cと同一であれば、レコーダ1は、正しいとしてメモリカード40を認める（すなわち、認証する）。この段階では、レコーダ1およびメモリカード40の両者が選択した認証キーIKjおよび乱数Sd、Smを有している。そして、レコーダ1は、ステップS6において、 $MAC(IKj, Rm//Rd)$ をセッションキーSekと指定する。メモリカード40側でも、 $MAC(IKj, Rm//Rd)$ をセッションキーSekと指定する。このように、正しく相互認証がなされると、セッションキーSekをレコーダ1とメモリカード40とが共有する。セッションキーは、認証が成立する度に生成される。

【0057】図11は、レコーダ1によりオーディオフィールをメモリカード40のフラッシュメモリ42に記

録する時のキーの書き込み処理を示す。なお、書き込み処理を開始するときには、セッションキーSekの生成処理が終了しており、セッションキーSekをレコーダ1とメモリカード40とが共有している。ステップS11において、レコーダ1は、コンテンツのトラックデータ毎に乱数を発生し、乱数に応じてコンテンツキーCKを作成する。次に、ステップS12において、レコーダ1は、コンテンツキーCKをセッションキーSekで暗号化し、暗号化したDES (Sek, CK) をメモリカード40に送信する。

【0058】メモリカード40は、ステップS13において、このデータを受け取り、セッションキーでコンテンツキーCKを復号する。すなわち、IDES (Sek, DES (Sek, CK)) と復号処理が表記される。次のステップS14において、メモリカード40は、復号したコンテンツキーCKをメモリカード40のストレージキーKstmで再度、暗号化し、再暗号化したコンテンツキーDES (Kstm, CK) がレコーダ1に送信される。

【0059】レコーダ1は、ステップS15において、再暗号化したコンテンツキーを、パーツデータエリア112を管理するキーエリア111に配置させ、再暗号化されたコンテンツキーCKおよびコンテンツがメモリカード40のフラッシュメモリに記録されるようにフォーマット化の処理を行う。コンテンツの暗号化のために、図9に示されるように、コンテンツキーCKとパーツキーPKとの排他的論理和または論理積がとられる。その結果、テンポラリーキーTMKが得られる。テンポラリーキーTMKは、セキュリティブロック3内にのみ存在し、外部からはアクセス可能ではない。各ブロック113の先頭で乱数を発生し、これをブロックシードBK、SEEDとし、各パーツデータエリア112内に格納される。レコーダ1は、テンポラリーキーTMKでブロックシードBK、SEEDを暗号化し、ブロックキーBKが得られる。すなわち、 $BK = (CK (+) PK, BK \text{ SEED})$ の関係が得られる。ブロックキーBKもセキュリティブロック3内にのみ存在し、セキュリティブロック3の外部からはアクセス可能ではない。

【0060】ステップS16において、レコーダ1は、ブロックキーBKによってパーツデータエリア112内のデータをブロック毎に暗号化し、暗号化されたデータと、キーエリア111内のデータをメモリカード40に送信する。メモリカード40は、レコーダ1から受け取った暗号化されたデータおよびキーエリア111内のデータ（ヘッダデータ）をフラッシュメモリ42に記録する（ステップS17）。

【0061】図12は、レコーダ1がメモリカード40のフラッシュメモリ42に蓄えられているオーディオトラックを再生する時の処理の流れを説明するために、簡略化したブロック図であり、図1と対応する部分には、

同一符号を付して示し、暗号化および復号化の説明に特に不要な構成は、省略されている。図13は、図12と同様に、レコーダ1によりオーディオトラックをメモリカード40のフラッシュメモリ42から再生する時の復号化処理を示す。再生時でも、相互認証が成立することによって、レコーダ1とメモリカード40との間でセッションキーSekが共有される。

【0062】ステップS21において、レコーダ1は、メモリカード40からデータ読み出すことによって、ストレージキーKstmで暗号化されたコンテンツキーCKすなわち、 $(DES (Kstm, CK))$ と、暗号化されたコンテンツ（所望のトラックのパーツデータエリア102）を得る。そして、レコーダ1は、ストレージキーKstmで暗号化されたコンテンツキーCKをメモリカード40に渡す。

【0063】ステップS22において、メモリカード40は、ストレージキーKstmでコンテンツキーCKを復号する（ $IDES (Kstm, DES (Kstm, CK))$ ）。ステップS23において、メモリカード40は、復号したコンテンツキーをセッションキーSekで暗号化し、 $DES (Sek, CK)$ をレコーダ1に送る。

【0064】レコーダ1は、ステップS24において、セッションキーSekでコンテンツキーを復号する。次のステップS25において、レコーダ1は、復号したコンテンツキーCKと、パーツキーPKと、ブロックシードBK、SEEDを使用してブロックキーBKを作成する。ステップS26では、レコーダ1は、ブロック毎にブロックキーBKによって暗号化されたパーツデータエリア102をそれぞれ復号化する。復号化されたオーディオデータがオーディオエンコーダ／デコーダ7によって復号化される。

【0065】上述した読み出し動作、書き込み動作以外においても、状態1において、コマンドが伝送され、その後の状態2において、コマンドに対応するデータが伝送される。レコーダ1とメモリカード40間のシリアルインタフェースは、上述したものに限定されず、種々のものを使用できる。

【0066】この発明の一実施形態におけるレコーダ1とメモリカード40との間のシリアルインタフェースについてより詳細に説明する。図2に示されるように、レコーダ1とメモリカード40との間を結合する10本の線の内、信号の送受信にとって主要なものは、クロック線SCK、ステータス線SBSおよびデータ線DIOである。

【0067】図14は、メモリカード40からデータを読み出す時のタイミングを示す。状態0（初期状態）以外の状態において、クロック線SCKを介して伝送されるデータと同期したクロックが伝送される。レコーダ1とメモリカード40との間で、何等データの送受信がさ

れていない状態では、ステータス線SBSがローレベルとなっている。これが状態0（初期状態）である。そして、タイミングt31において、レコーダ1がステータス線SBSをハイレベルとし、状態1となる。

【0068】メモリカード40（S/P、P/S、IFブロック43）は、ステータス線SBSがハイレベルに切り替わったことによって、状態0から状態1へ変化したことを検出する。状態1では、データ線DIOを介してレコーダ1からメモリカード40に対して読み出しコマンドが送信され、メモリカード40が読み出しコマンドを受信する。この読み出しコマンドは、シリアルインタフェース用のTPC（Serial Protocol Command）と称されるプロトコルコマンドである。後述するように、プロトコルコマンドによって、通信の内容と後続するデータのデータ長が特定される。

【0069】コマンドの送信が完了したタイミングt32において、ステータス線SBSがハイレベルからローレベルに切り替えられる。それによって、状態1から状態2へ遷移する。状態2では、メモリカード40が受信したコマンドで指示される処理、具体的には、読み出しコマンドで指定されたアドレスのデータをフラッシュメモリ42から読み出す処理を行う。この処理がなされている間、データ線DIOを介してビジー信号（ハイレベル）がレコーダ1に送信される。

【0070】そして、フラッシュメモリ42からデータの読み出しが完了したタイミングt33において、ビジー信号の出力が停止され、レコーダ1に対してメモリカード40からデータを送出する準備ができたことを示すレディー信号（ローレベル）の出力が開始される。

【0071】レコーダ1は、メモリカード40からレディー信号を受信することによって、読み出しコマンドに対応する処理が準備できたことを知り、タイミングt34において、ステータス線SBSをハイレベルに切り替える。すなわち、状態2から状態3へ遷移する。

【0072】状態3になると、メモリカード40は、状態2においてページバッファ45に読み出したデータをデータ線DIOを介してレコーダ1に対して出力する。読み出しデータの転送が完了したタイミングt35において、レコーダ1は、クロック線SCKを介して伝送されていたクロックの供給を停止すると共に、ステータス線をハイレベルからローレベルへ切り替える。それによって、状態3から初期状態（状態0）に遷移する。

【0073】なお、メモリカード40の内部状態に変化が生じて何らかの割り込み処理を行う必要が発生すると、メモリカード40は、タイミングt36で示すように、状態0において、割り込みを示すインターラプト信号をデータ線DIOを介してレコーダ1に供給する。レコーダ1は、状態0でメモリカード40からデータ線DIOを介して信号が供給された場合、その信号がインターラプト信号であることを認識できるように設定されて

いる。レコーダ1がインターラプト信号を受け取ると、そのインターラプト信号に基づいて必要な処理を行う。

【0074】図15は、メモリカード40のフラッシュメモリ42に対してデータを書き込む時のタイミングチャートである。初期状態（状態0）では、クロックSCKの伝送がされない。タイミングt41において、レコーダ1がステータス線SBSをローレベルからハイレベルに切り替える。それによって、データ線DIOを介して書き込みコマンドが伝送される状態1に遷移する。メモリカード40は、状態1において、コマンドを取得するように準備する。タイミングt41からコマンドがデータ線DIOを介してメモリカード40に伝送され、メモリカード40がこの書き込みコマンドを取得する。

【0075】書き込みコマンドの送信が完了したタイミングt42において、レコーダ1がステータス線SBSをハイレベルからローレベルに切り替える。それによって、状態1から状態2へ遷移する。状態2では、レコーダ1が書き込みデータをデータ線DIOを介してメモリカード40に伝送する。メモリカード40では、受け取った書き込みデータがページバッファ45に蓄えられる。

【0076】書き込みデータの伝送が終了するタイミングt43において、ステータス線SBSがローレベルからハイレベルへ切り替えられ、状態2から状態3へ遷移する。状態3において、メモリカード40は、書き込みデータをフラッシュメモリ42へ書き込む処理を行う。状態3において、メモリカード40は、データ線SBSを介してビジー信号（ハイレベル）をレコーダ1に対して送信する。レコーダ1は、書き込みコマンドを送信し、且つ現在の状態が状態3であることから、メモリカード40から送信される信号がステータス信号であると判断する。

【0077】メモリカード40において、書き込みデータの書き込み処理が終了すると、終了したタイミングt44において、ビジー信号の出力を停止し、レディー信号（ローレベル）をレコーダ1に対して送信する。レコーダ1は、レディー信号を受信すると、書き込みコマンドに対応する書き込み処理が完了したものと判断し、クロック信号の送信を止めると共に、タイミングt45においてステータス線SBSをハイレベルからローレベルへ切り替える。それによって、状態3から状態0（初期状態）に戻る。

【0078】さらに、状態0において、メモリカード40からデータ線DIOを介してハイレベルの信号をレコーダ1が受け取った場合には、レコーダ1がこの信号をインターラプト信号と認識する。そして、レコーダ1は、受信したインターラプト信号に基づいて必要な処理を行う。例えばメモリカード40をレコーダ1から取り外した時に、メモリカード40がインターラプト信号が発生する。

【0079】上述した読み出し動作、書き込み動作以外においても、状態1において、コマンドが伝送され、その後の状態2において、コマンドに対応するデータが伝送される。レコーダ1とメモリカード40間のシリアルインタフェースは、上述したものに限定されず、種々のものを使用できる。

【0080】この発明の一実施形態において、メモリカードを使用できる機器によりなされる処理について図16を参照してより詳細に説明する。機器の電源がオンされると（ステップS200）、ステップS201でメモリカードが挿入されているかどうかが決まる。メモリカードが挿入されていると決定されると、メモリカードのブートブロックが読み込まれる（ステップS202）。

【0081】図7を参照して説明したように、ブートブロックのブート&アトリビュート情報中には、セキュリティ対応かどうかの識別情報が含まれている。この識別情報を参照して、挿入されたメモリカードがセキュリティ対応か、非対応かが決定される（ステップS203）。セキュリティ対応のメモリカード40であれば、ステップS204において、認証動作がなされ、認証成立後にコンテンツデータの記録／再生がなされる（ステップS205）。

【0082】ステップS203において、挿入されたメモリカードがセキュリティ非対応のメモリカード40'であると決定されると、ステップS206において、挿入したメモリカード40'が使用できない旨の告知がなされる。表示デバイス5上で警告メッセージを表示することによって、告知がなされる。音声等の他の方法によって告知を行っても良い。

【0083】上述した処理は、レコーダ1のように、セキュリティ対応の機器が行うものである。若し、機器がセキュリティ非対応の場合には、図16において破線で示すように、ステップS202（ブートブロックの読み込み）の後に、ステップS207に処理が移る。ステップS207では、挿入されたメモリカードがセキュリティ対応か、非対応かが決定される。ステップS207における決定の結果が肯定、否定の何れであっても、ステップS208およびS209で示すように、メモリカード40'に対して、通常動作（書き込み、読み出し、消去等）を行うことができる。

【0084】以上説明した一実施形態では、メモリカードの機能がセキュリティ機能であったが、この発明は、セキュリティ機能に限定されるものではない。例えば機器とメモリカードとのインタフェースにおける通信速度またはデータレートが既存の速度（低速）より速い速度（高速）が可能とされる。この速度に関しての新機能をメモリカードが持つ場合に対して、この発明を適用できる。

【0085】図17は、速度に関する処理を示すフロー

チャートである。ステップS300で電源がオンされ、ステップS301でメモリカードが挿入されたかどうかが決まり、ステップS302でブートブロックが読み込まれる。ブロックブロック中には、セキュリティ機能と同様に、そのメモリカードが高速対応か、非対応かの識別情報が含まれている。

【0086】この識別情報によって、メモリカードが高速対応と決定すれば、機器とメモリカード間の通信速度またはデータレートを低速から高速へ切り替え（ステップS304）、高速動作がなされる（ステップS305）。若し、ステップS303において、高速非対応と決定されると、低速動作がなされる（ステップS306）。機器が高速非対応の場合には、図17において破線で示すように、高速対応かどうかの決定（ステップS307）の結果に影響されずに、低速動作がなされる（ステップS308およびS309）。

【0087】なお、上述した説明では、DESを使用した場合を説明したが、セキュリティのための方式としては、DESに限らず、種々の暗号化技術を採用することが多能である。

【0088】

【発明の効果】この発明によれば、メモリカードのように着脱自在のメモリ装置として、新機能を有するものと、それを有しないものとが混在していても、装着時に新機能の有無を機器が瞬時に決定することができる。従って、実際に機器がメモリカードと通信を行ってエラーとなるかどうかによって、新機能の有無を決定する方法と異なり、無駄な動作を生じることがない。また、メモリ装置の形状によって、新機能の有無を識別する方法と異なり、新機能を有するメモリカードを新機能に対応していない機器によって使用することが可能となり、メモリカードの互換性の点で有利である。

【図面の簡単な説明】

【図1】この発明の一実施形態の全体的構成を示すブロック図である。

【図2】この発明の一実施形態におけるセキュリティ対応のメモリカードの構成を示すブロック図である。

【図3】この発明の一実施形態におけるセキュリティ非対応のメモリカードの構成を示すブロック図である。

【図4】この発明の一実施形態におけるフラッシュメモリのファイルシステム処理階層の構成を示す略線図である。

【図5】この発明の一実施形態におけるフラッシュメモリのデータの物理的構成のフォーマットを示す略線図である。

【図6】フラッシュメモリのブートブロックの構成を示す略線図である。

【図7】フラッシュメモリのブートブロックのブートおよびアトリビュート情報の構成を示す略線図である。

【図8】この発明の一実施形態におけるコンテンツにお

けるキーの関係を示す略線図である。

【図9】この発明の一実施形態における録音時の暗号化処理を説明するためのブロック図である。

【図10】この発明の一実施形態における認証処理を説明するための略線図である。

【図11】この発明の一実施形態における録音時の暗号化処理を説明するための略線図である。

【図12】この発明の一実施形態における再生時の暗号化処理を説明するためのブロック図である。

【図13】この発明の一実施形態における再生時の暗号化処理を説明するための略線図である。

【図14】この発明の一実施形態におけるレコーダとメモリカード間のインタフェースを説明するためのタイミングチャートである。

【図15】この発明の一実施形態におけるレコーダとメ

モリカード間のインタフェースを説明するためのタイミングチャートである。

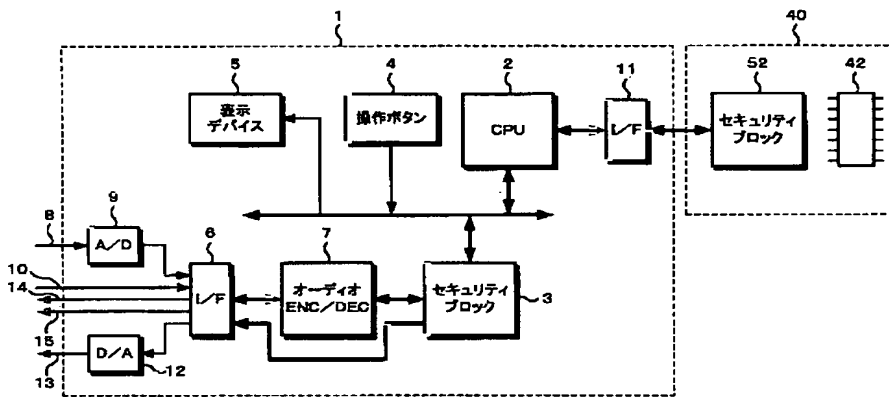
【図16】この発明の一実施形態の動作説明に用いるフローチャートである。

【図17】この発明をセキュリティ機能以外の機能に対して適用した例を説明するためのフローチャートである。

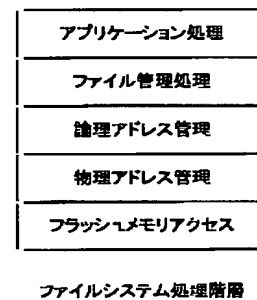
【符号の説明】

1・・・レコーダ、2・・・CPU、3・・・セキュリティブロック、7・・・オーディオエンコーダ/デコーダ、11・・・メモリインタフェース、40・・・セキュリティ対応のメモリカード、40'・・・セキュリティ非対応のメモリカード、43・・・S/P、P/S、I/Fブロック、42・・・フラッシュメモリ、52・・・セキュリティブロック

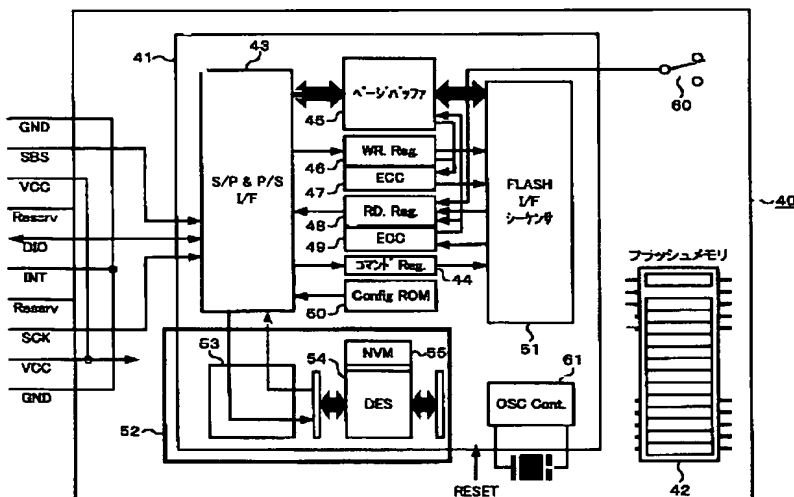
【図1】



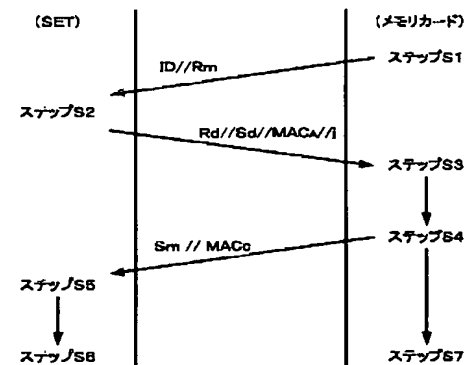
【図4】



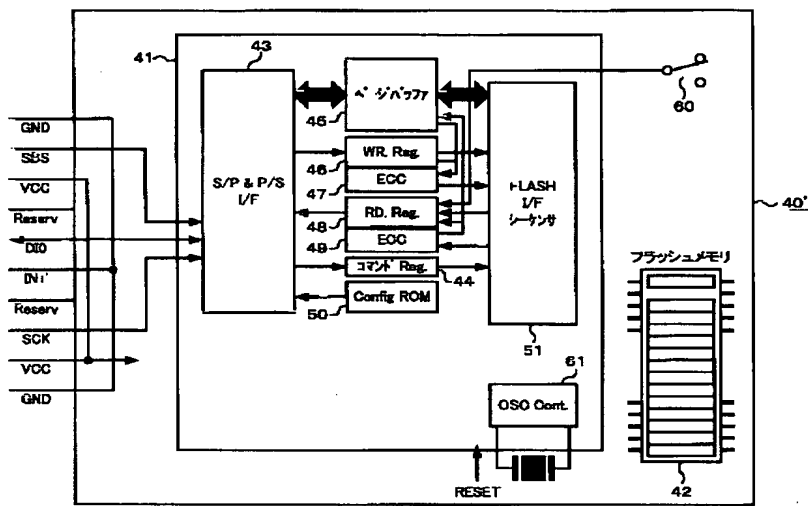
【図2】



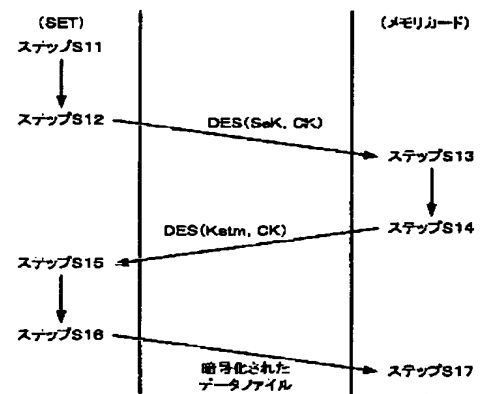
【図10】



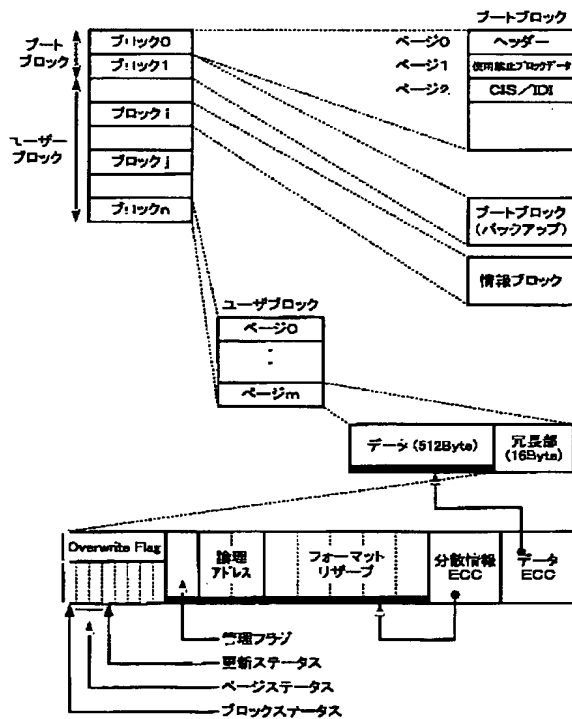
【図3】



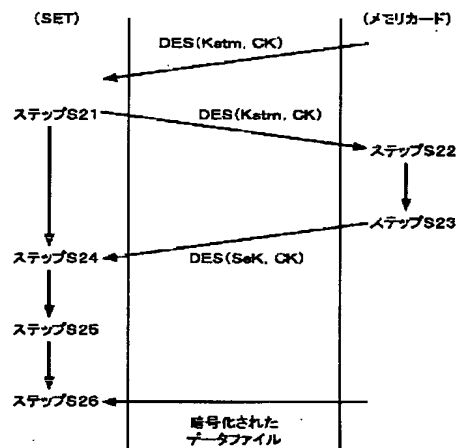
【図11】



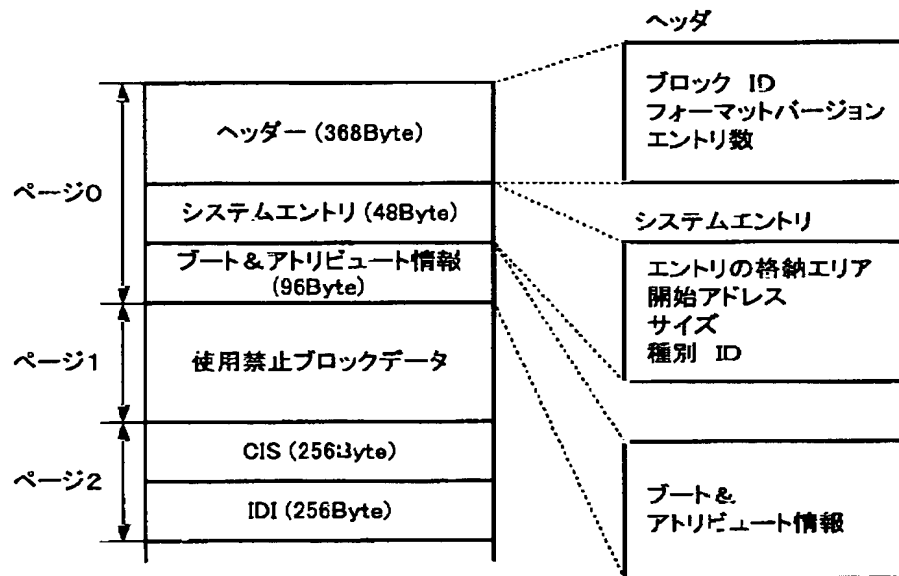
【図5】



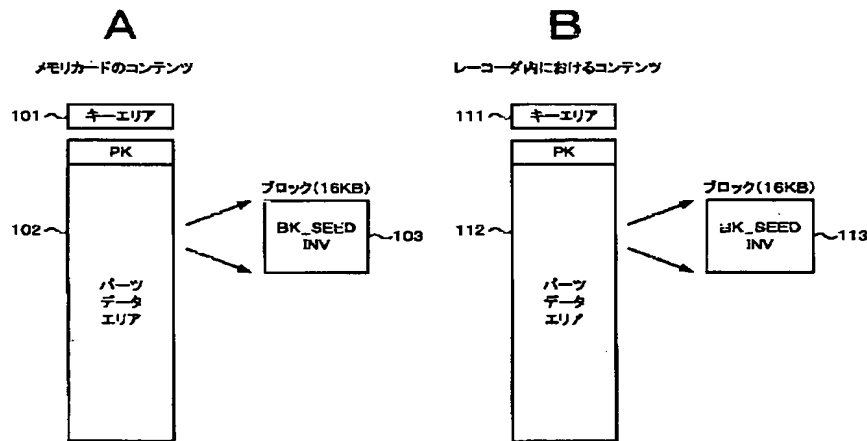
【図13】



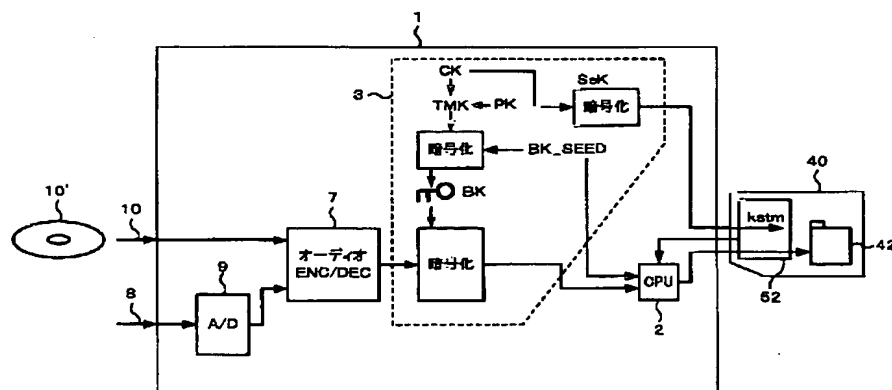
【図6】



【図8】



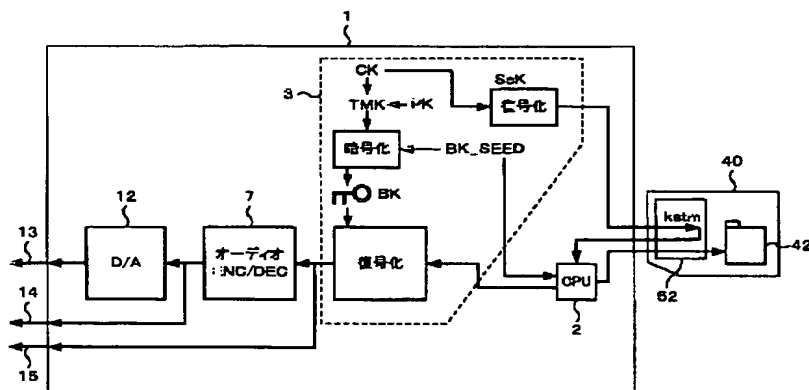
【図9】



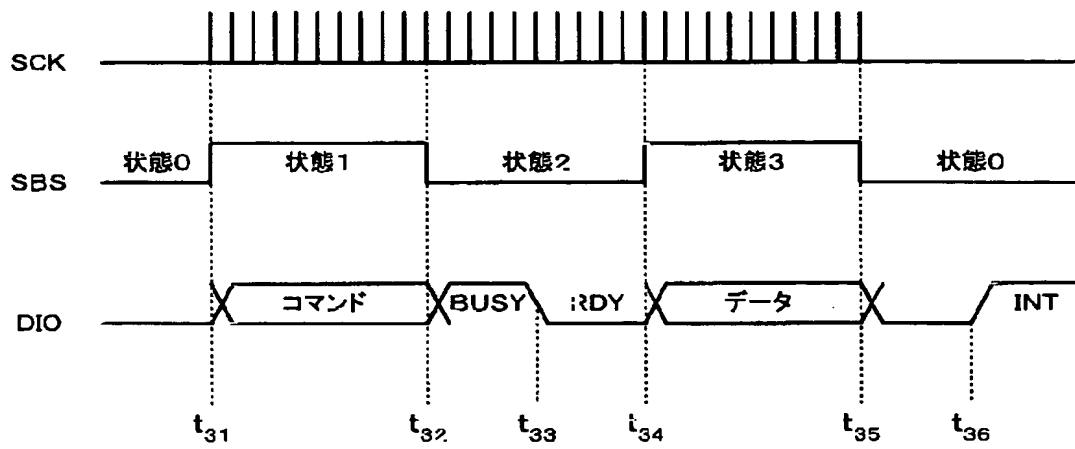
【図7】

バイト数	
MS クラス (*1)	1 1:Type-1 Other reserved
カードタイプ (*1)	1 1:Read Only 2:Read Write 3:Hybrid Other reserved
ブロックサイズ (*1)	2 KB単位でブロックサイズを表現 16KB:0x0010 8KB:0x0008
ブロック数 (*1)	2 ブロック数
総ブロック数 (*1)	2 総ブロックの数
ページサイズ	2 ページサイズは12固定0x0200
冗長部サイズ	1 冗長部サイズ16バイトの場合0x10
セキュリティ対応 (*1)	1
アセンブリ日時 (*2)	8 カード(ハード)の作成年月日 (次ページ日時指定フォーマット参照)
事業所エリア (*2)	4 シリアル番号等の事業所管理に使用
MS アセンブリメーカーコード (*2)	1 登録のアセンブリメーカーコード
MS アセンブリ機種コード (*2)	3 登録のアセンブリ機種コード
メモリメーカーコード	2 チップのメーカーコード 0:不明
メモリデバイスコード	2 デバイスコード 0:不明
メモリサイズ	2 MByte数を記述ex) 32Mbit Flash 0x0004
フォーマットリザーブ	1 1を設定 Other reserved
フォーマットリザーブ	1 1を設定 Other reserved
VCC	1 VCC単位0.1Vで表現ex) 3.3V 0x21
VPP	1 VPP単位0.1Vで表現ex) 3.3V 0x21
コントローラ番号	2 コントローラチップ番号
リザーブ	14
フォーマット種別 (*1)	1 1:FAI Other reserved
用途	1 0:汎用 Other reserved
ゼロリセットリザーブ	5
リザーブ	35

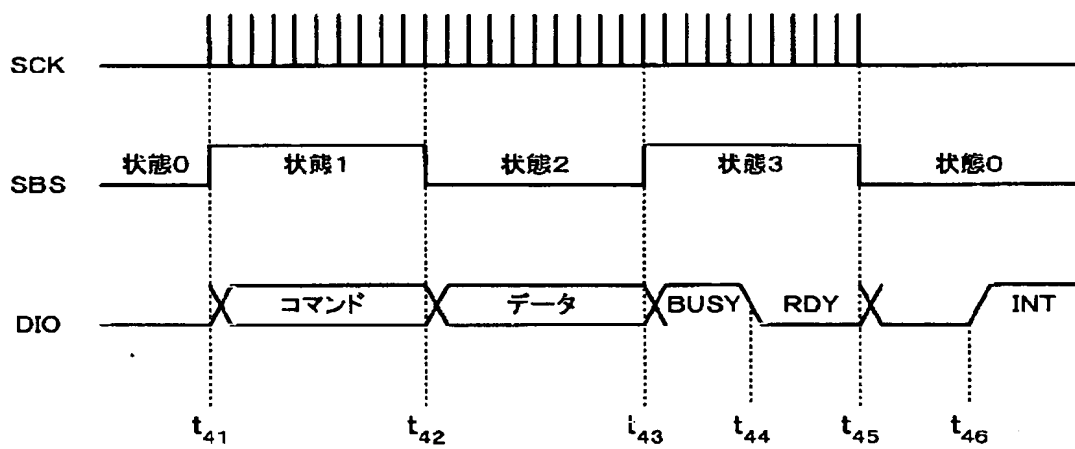
【図12】



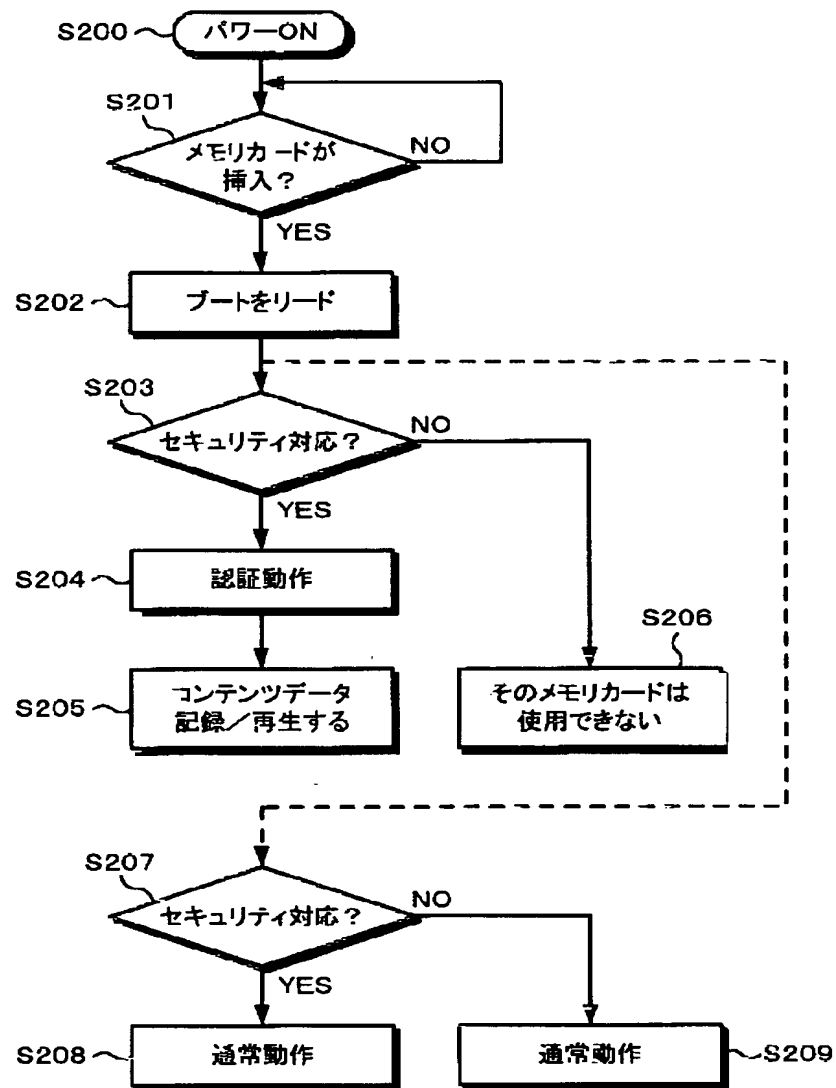
【図14】



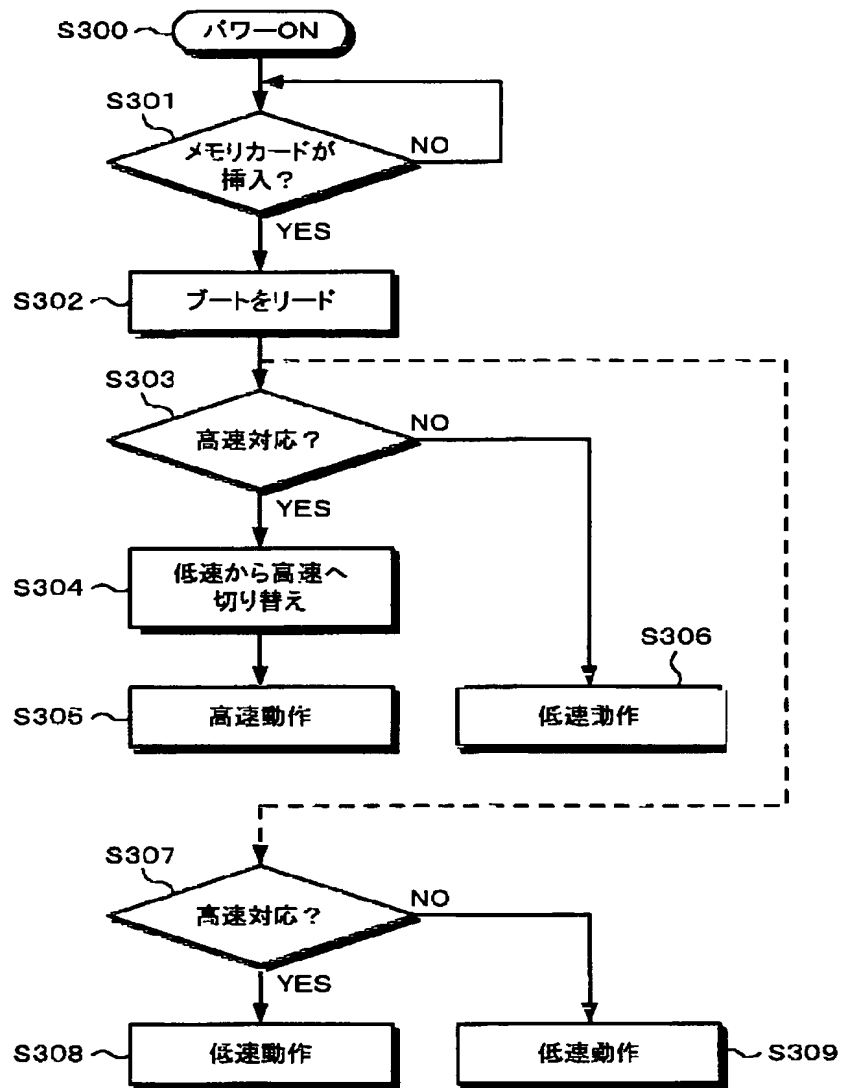
【図15】



【図16】



【図17】



フロントページの続き

(51)Int. Cl.⁷

H04L 9/10

識別記号

F I

G10L 9/18

H04L 9/00

J

621A

(参考)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.